AUSA: Timothy Wyse Telephone: (313) 226-9144

AO 91 (Rev. 11/11) Criminal Complaint Special Agent: Mike Bertrand(FBI) Telephone: (313) 965-2323

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

United States of America
v.

Jibreel Darnell Pratt

Case No. Case: 2:23−mj−30352
Assigned To : Unassigned
Assign. Date : 8/25/2023
Description: RE: SEALED MATTER (EOB)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of December 2019 and July 2021 in the county of Wayne and elsewhere in the Eastern District of Michigan, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1028(a)(7) 18 U.S.C. § 1029(a)(2)	Possession of means of identification in connection with another felony offense, including wire fraud.
18 U.S.C. § 1029(a)(3)	Use and trafficking of access devices.
18 U.S.C. § 1030(a)(2)	Possession of 15 or more access devices.
18 U.S.C. §1030(b); 18 U.S.C §1343	Illegally accessing a protected computer. Conspiracy to commit computer fraud; wire fraud.

This criminal complaint is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Mike Bertrand, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Date: August 25, 2023

Judge's signature

City and state: Ann Arbor, MI

Hon. David R. Grand, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Michael Bertrand, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for issuance of a criminal complaint and arrest warrant for JIBREEL DARNELL PRATT.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so since 2022. I am currently assigned to the FBI's Detroit Cyber Division. My current duties concern investigating crimes involving computer fraud, wire fraud, identity theft, money laundering, and conspiracies to commit those crimes. I have a Bachelor of Arts Degree in Philosophy, a Master's Degree in Philosophy, a Doctoral Degree in Philosophy and approximately ten years of professional experience as a university philosophy professor. Additionally, I have received specialized training in the FBI relevant to the investigation of computer-related crimes.

3. This affidavit is based upon information supplied to me by other law enforcement officers, including other Special Agents employed by the FBI. It is also based upon my personal involvement in this investigation and on my training and experience. In submitting this affidavit, I have not included every fact known to me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause to support this application for issuance of an arrest warrant.

4. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices);

1030(a)(2) (illegally accessing a protected computer); 1030(b) (conspiracy to commit computer fraud); and 1343 (wire fraud), have been committed by JIBREEL DARNELL PRATT.

PROBABLE CAUSE

Background Regarding the Genesis Market Investigation

5. Since August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market.[1] Genesis Market is primarily hosted at the Internet domain "genesis.market."[2] Genesis Market's operators compile stolen data (*e.g.*, computer and mobile device identifiers, email addresses, usernames, and passwords) from malware-infected[3] computers around the globe and package it for sale on the market.[4] Genesis Market has been the subject of various cybersecurity presentations and news stories. For example, CBS News ran a story on Genesis Market in September 2021.[5]

---

[1] On April 4, 2023, the FBI and its partners dismantled Genesis Market and arrested many of its users around the world. See Department of Justice Office of Public Affairs, *Criminal Marketplace Disrupted in International Cyber Operation*," April 5, 2023, available at www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation/ (last visited 4/5/2023).

[2] A domain name is a way to identify computers on the Internet, using a series of characters that correspond with a particular IP address. Genesis Market is also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains include the website "g3n3sis.org," as well as the TOR domain "genesiswiwn7p7lmbvimup7v767e64rcw6o3kfcnobu3nxisteprx2qd.onion." TOR is short for "The Onion Router" and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user.

[3] Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

[4] Genesis Market refers to these packages of stolen data as "bots" on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market's use of the word "bot" strays from the normal meaning, the term "package" is used throughout this request.

[5] See Dan Patterson, *Inside Genesis: The market created by cybercriminals to make millions selling your digital identity*, September 9, 2021, available at https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/ (last visited 12/19/2022).

6. The packages advertised for sale on Genesis Market vary by price and many packages are available for around $10 to $20 per package. The price appears to vary based on three primary factors: (1) the number of online accounts ("resources") associated with the package (e.g., accounts with legitimate credentials for platforms like Amazon, Netflix, Gmail, etc. are more valuable); (2) how recently the package was compromised with malware; and (3) whether there is a "fingerprint" associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary plugin (i.e., an Internet browser extension that provides additional functionality). This proprietary plugin amplifies that purchaser's ability to control and access the package's data and masquerade as the victim device.

7. Genesis Market's operators have advertised Genesis Market on prominent online criminal forums, including exploit.in and xss.is. Those advertisements include news, updates, and information regarding Genesis Market. For example, the advertisements have included (1) information about packages for sale on Genesis Market; (2) specific replies to users requesting packages located in specific countries; and (3) updates regarding the tools available through Genesis Market.

8. Genesis Market users can gain initial access to Genesis Market via an invitation from a Genesis Market operator on a cybercriminal forum, or via an invitation from an individual who already has an account on Genesis Market. The invitations are for one-time use and in the form of an alphanumeric text string. Once a prospective new user receives an invitation, the new user can go to a Genesis Market domain to create a username and password. Genesis Market then

requests the new user to associate their Jabber ID or email address with that new account.[6] Analysis by law enforcement has found that a Jabber ID or email address is not absolutely required when registering an account, nor is the Jabber ID or email address verified by Genesis Market administrators. Nonetheless, the vast majority of Genesis users have registered with a Jabber ID or email address, as it is one of the fields to enter registration data when creating a new account.

9. While conducting covert operations, law enforcement has observed that for new users logged into Genesis Market, the front page generally displays a "dashboard" of information, including the number of packages listed for sale and a "Genesis Wiki" page that walks a new user through Genesis Market's platform and how to use it. Below is a screenshot taken April 1, 2021, of the front page of Genesis Market.[7] The front page displays the total amount of "bots" (packages) available for sale on Genesis Market at that time, categorized by country. This page appears immediately after the user logs into his or her account. The tabs on the left allow for the Genesis Market user to traverse the market:

[6] Jabber is a chat and communications platform akin to AOL Instant Messenger. It is prominent among cybercriminal operators because it is considered exceptionally secure.

[7] Portions of the screenshots in this affidavit have been redacted or omitted to conceal information that might identify accounts used covertly by investigators.